DEC STD 139-0 Reliability Prediction and Assessment

DOCUMENT IDENTIFIER: A-DS-EL00139-00-0000 Rev B, 24-Jun-1991

ABSTRACT: This standard defines the policies, procedures, processes and tools recommended for reliability prediction and assessment of Digital products in support of customer satisfaction goals. Note: This revision does not include software.

APPLICABILITY: This standard is applicable to all networks, clusters, systems, options, and components that are developed or purchased (buyouts) by Digital, including all the hardware, firmware, and software products that form the building blocks.

STATUS: APPROVED 24-Jun-1991; use VTX SMC for current status.

This document is confidential and proprietary, and is the property of Digital Equipment Corporation. It is an unpublished work protected under the Federal copyright laws.

© Digital Equipment Corporation. 1991. All rights reserved.

DEC STD 139-0 Reliability Prediction and Assessment

DOCUMENT IDENTIFIER: A-DS-EL00139-00-0000 Rev B, 24-Jun-1991

REVISION HISTORY:	Rev A,	22-Jan-1976	
	Rev B,	24-Jun-1991	ECO Number CTS01

Document Management Category:	Reliability Testing (HTR)
Responsible Department:	Reliability Assessment Committee (RAC)
Responsible Person:	Gary Kushner
SMC Writer:	Eric Falkof

APPROVAL: This document has been reviewed and recommended for approval by the General Review group for its category.

Gary Kushner - Systems Reliability Engineering

Eric Williams - Standards Process Manager

Direct requests for further information to:

George Borrero
Use $ VTX ELF for the latest location information.

Use VTX SMC to order copies of this document from Standards and Methods Control. Send distribution questions to JOKUR::SMC or call DTN: 234-4423.

CONTENTS

1 INTRODUCTION 1
1.1 SCOPE 1
1.2 POLICY 1
1.3 RESPONSIBILITIES 2
1.4 DEFINITIONS 2
1.4.1 Prediction 2
1.4.2 Assessment 3

2 CONTEXT OF RELIABILITY PREDICTION, ASSESSMENT, AND FEEDBACK (RPAF) IN THE OVERALL RELIABILITY PLANNING FOR DIGITAL 4
2.1 RELIABILITY GOALS AND REQUIREMENTS 4
2.2 LEVELS OF APPLICATION 5
2.3 RELIABILITY PREDICTION 6
2.4 RELIABILITY TRADEOFF AND IMPACT ANALYSIS 6
2.5 RELIABILITY ASSESSMENT 6
2.6 RELIABILITY FEEDBACK 7
2.7 RELIABILITY PLANNING PROCESS 7

3 RELIABILITY PREDICTION AND ASSESSMENT REQUIREMENTS 8
3.1 GENERAL REQUIREMENTS 8
3.2 RELIABILITY MODELING 9
3.2.1 Hardware Failure Rate 10
3.2.2 Interruption Rate and Availability 11
3.2.2.1 Fault Occurrence and Error-Handling Submodels 12
3.3 FAILURE DATA SOURCES 13
3.3.1 Prediction Data 13
3.3.2 Data Collection Considerations 13
3.4 PREDICTION AND ASSESSMENT PROCEDURE 14
3.5 DONENESS CRITERION 15
3.6 TOOLS 15
3.6.1 Hardware Failure Rate Prediction 15
3.6.2 Hardware Failure Rate Assessment 16
3.6.3 Interruption Rate and Availability Prediction and Assessment 16

Appendix A REFERENCED DOCUMENTS 17
A.1 EL-Class Digital Documents 17
A.2 Other Digital Documents 17

Appendix B RELATED DOCUMENTS 19
B.1 EL-Class Digital Documents 19
B.2 Other Documents 19
B.3 Ordering Information 19

Appendix C BIBLIOGRAPHY 21

GLOSSARY 23

FIGURES

1 Context of RPAF in the Reliability Program Plan 4
2 Levels of Application for Prediction, Assessment, and Feedback 5

1 INTRODUCTION

This standard defines the policies, procedures, processes and tools recommended for reliability prediction and assessment of Digital products in support of customer satisfaction goals.

The intent is to define the essential elements and a process so reliability predictions and assessments are consistent to fulfill all requirements. There is an emphasis on common language, definitions, and methods.

The standard describes the processes to follow to determine reliability and availability requirements. The standard describes a set of requirements to be used by all persons or product teams for reliability prediction, assessment, and feedback activities over the development life cycle and product useful life.

In this standard, the term reliability is used in its broadest sense to include the concepts of reliability and availability, failures and interruptions, and cause and effect relationships.

This standard is not intended to provide detailed procedures nor does it mandate the use of any specific reliability tool or method.

1.1 SCOPE

This standard is applicable to all networks, clusters, systems, options, and components that are developed or purchased (*buyout*) by Digital, including all the hardware, firmware, and software products that form the building blocks.

Revision C of this standard will contain software design for reliability.

The primary users of this standard are reliability and quality engineers, hardware and software product designers, manufacturing engineers, CSSE maintainability engineers, and customer service logistics engineers. The secondary users include marketing and sales personnel, and, when there are proprietary agreements, Digital customers and vendors.

1.2 POLICY

It is Digital policy "to design, produce, deliver, and support products that meet quality standards and perform reliably in the customer's application" (Kenneth H. Olsen, *Digital Quality Systems*).

1.3 RESPONSIBILITIES

Product Manager–

The Product Manager is responsible for ensuring that the reliability requirements are clearly identified in the Product Specification, and that they are competitive in meeting customer requirements.

Product Marketing Manager–

The Product Marketing Manager is responsible for providing aggressive reliability goals to enhance Digital's competitive position.

Customer Service and Systems Engineering (CSSE)–

The CSSE organization is responsible for ensuring that the product reliability requirements meet or exceed the service delivery and service financial goals and for assisting the Product Team in the reliability specification and assessment consistent with this standard.

Manufacturing Program Manager–

The Manufacturing Program Manager is responsible for ensuring that the product meets or exceeds the requirements of this standard on a continual basis.

Product Team–

Members of the Product Team are responsible for ensuring that the reliability prediction and assessment are consistent with the requirements delineated in this standard. Responsibility for developing and maintaining reliability prediction and assessment models is also a responsibility of the Team. The Product Team implements this under the overall direction of the above.

1.4 DEFINITIONS

This section defines the terms *prediction* and *assessment*.

1.4.1 Prediction

Reliability prediction is a forecast of expected reliability performance for the purpose of judging whether or not some action is required. Some typical decisions based on reliability prediction include the following:

- To make comparisons with requirements, to determine the ability of products, systems, and services to meet specified market and business requirements
- To identify areas requiring reliability improvements through the allocation of requirements to subsystems
- To make business decisions, to evaluate the cost-effectiveness of various design, maintenance, and logistic support alternatives

The effective use of reliability prediction methods accurately identifies the areas for improvement early enough in the design process to ensure business objectives (that is, time to market, performance, cost) can be met.

1.4.2 Assessment

Reliability assessment is an evaluation of observed (actual) reliability performance of a sample of units for the purpose of judging whether or not some action is required. Typical decisions based on reliability assessment include the following:

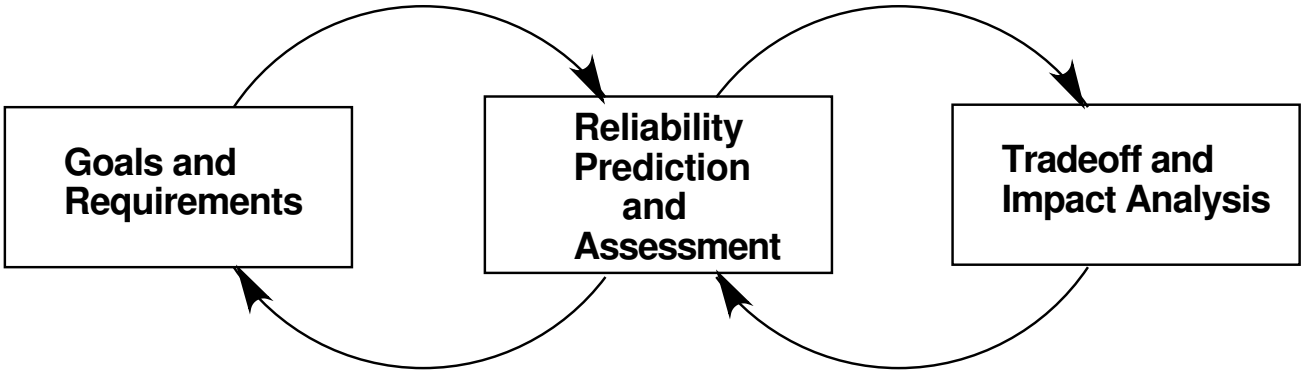
- To demonstrate reliability, in conformance with the Phase 3 Exit criteria from Reliability Qualification Test (RQT) and Process Verification Test (PVT)
- To evaluate the effectiveness of infancy reduction procedures (for example, burn-in or other stress screens), to establish the provisions for warranty policies, and to determine the spares allocations for customer service logistics management
- To measure reliability in manufacturing Ongoing Reliability Test (ORT) and in field use, and to compare the measurements to goals
- To make comparisons in the feedback loop between assessments and predictions and to validate underlying distributional assumptions

The effective use of reliability assessment methods simultaneously measures reliability and drives failure analysis and corrective action.

2 CONTEXT OF RELIABILITY PREDICTION, ASSESSMENT, AND FEEDBACK (RPAF) IN THE OVERALL RELIABILITY PLANNING FOR DIGITAL

The Reliability Program Plan [1]* , written in Phase 0, describes the specific and detailed plan for reliability for each new product or family of products. The context of RPAF in the Reliability Program Plan is shown in Figure 1. The focus of DEC STD 139-0 is the reliability prediction and assessment activities. The activities involved in establishing reliability requirements and in performing tradeoff and impact analyses, are described in DEC STD 139-0 only for completeness.

Figure 1: Context of RPAF in the Reliability Program Plan



2.1 RELIABILITY GOALS AND REQUIREMENTS

A set of reliability goals are established in Phase 0 considering customer, technology, market, and competitive requirements. The design goals are set for the following parameters:

— Number of failures at the customer site in a specified interval (for example, failures in the first 1000 hours at the customer site)

— Mean time between failures (MTBF) at the customer site in the steady state period of operation (for example, the failure rate in a steady state period of operation at a customer site)

— Mean time to onset of the wearout period of operation

— Interruption rate at the customer site in a specified interval

— Availability (for example, percentage up time and other related metrics)

* The number in brackets refers to the Bibliography.

The reliability goals are then allocated among the major systems, options, and components, using structural and behavioral reliability models derived from the product architectural block diagram. The reliability models reflect the cause and effect relationships of the product design. Examples of reliability models include reliability block diagrams, fault trees, Markov models, and stochastic Petri Nets.

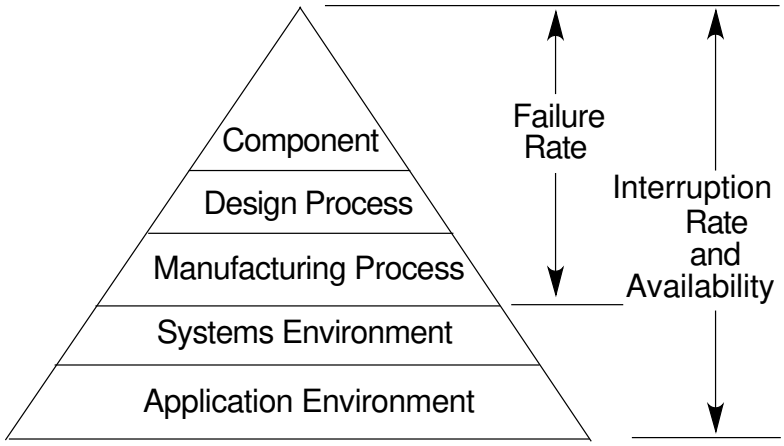
The major reliability tradeoff activity at the conceptual stage of the product design considers alternatives in the electrical, thermal, and architectural aspects of the design. This activity considers fault management techniques, and it provides the methods for achieving the reliability goals.

The reliability goals are used to establish requirements at the conclusion of the conceptual design process (Phase 1).

2.2 LEVELS OF APPLICATION

The levels of application for reliability prediction, assessment, and feedback are shown in Figure 2.* In this figure, component refers to either hardware (for example, CMOS semiconductor device, Head Disk Assembly or VAX™ kernel), or software (for example, VMS operating system). Systems environment refers to both hardware and software (for example, an 8974 VAXcluster™ running VMS™ Version 5.2). The application environment refers to the customer application running in the system or option. The application software can be developed by Digital, by the customer, or by a third party.

Figure 2: Levels of Application for Prediction, Assessment, and Feedback



* Derived from Ted Gent's conceptual model.

™ VAX, VAXcluster, and VMS are trademarks of Digital Equipment Corporation.

The prediction activity builds up from the component level, through the intermediate levels, to end at the application level. The assessment activity reverses this process, beginning with observed behavior at the application level and then breaking this down through root cause analysis to the other levels. The closed loop feedback of prediction and assessment is used to refine these activities.

The failure rate prediction typically is based on (generic) component knowledge and information on the (Digital) design and manufacturing processes. The failure rate assessment is observed at the design process level (Design Verification Test - DVT, Reliability Qualification Test - RQT) or the manufacturing process level (Process Verification Test - PVT, Ongoing Reliability Test - ORT). See *Digital Qualification Process Manual, EL-EN522-00* [2] and *Storage Systems Qualification Manual, EL-EN522-01* [3]. When failure rate data are observed at the systems or application environment levels, the assessment of component failure rate includes environmental effects that are not explicitly accounted for in the prediction activity.

The interruption rate and availability prediction is based on component knowledge, design and manufacturing information, and systems and application environmental effects. The assessment of interruption rate and availability typically is done at the application level, often at the customer site.

2.3 RELIABILITY PREDICTION

The reliability prediction is a forecast of expected reliability performance based upon a component list, architectural diagram, knowledge of the cause and effect relationships for the product(s), and operating environment. The reliability modeling techniques are used to forecast numerical values for the reliability goals described in Section 2.1. The reliability prediction activity is described in detail in Section 3.

2.4 RELIABILITY TRADEOFF AND IMPACT ANALYSIS

The reliability predictions continue to be refined as more precise design information becomes available. Product design and manufacturing process tradeoffs are evaluated to minimize cost and risk, while ensuring the reliability requirements are met. Areas evaluated include component integration, thermal management, stress screens, fault management techniques, and design for manufacturability. The cause and effect relationships are re-evaluated, the highest contributors are identified, and recommendations are made about how to minimize the impact on the product and process.

2.5 RELIABILITY ASSESSMENT

The reliability assessment is an evaluation of observed (actual) reliability performance based on the collection, analysis, and interpretation of reliability data. The data may be empirical or subjective (that is, Bayesian), or a combination of both. The analysis and interpretation activities are done in the context of a statistical assessment model, which itself is evaluated in terms of how well the data fit the underlying assumptions. The reliability assessment activity is described in detail in Section 3.

2.6 RELIABILITY FEEDBACK

The reliability feedback (loop) is a validation of the activities in the Reliability Program Plan, including the validity of the decisions made in the product design and manufacturing process areas.

The reliability assessment is compared to the reliability requirements. This comparison can result in another iteration of tradeoff and impact analysis, if necessary, to ensure the reliability requirements are met. The product design and manufacturing process decisions are then reviewed in the context of customer, technology, market, and competition. The objective is to improve the product design and manufacturing process in order to meet or exceed the reliability requirements.

The reliability assessment is also compared to the reliability prediction in terms of both the reliability metric values and the underlying statistical assumptions. This comparison is used to update the reliability databases, and, where necessary, to modify the statistical models. The objective is to adaptively update the RPAF methodology to ensure that reliability predictions are able to accurately forecast the reliability performance of products.

2.7 RELIABILITY PLANNING PROCESS

The activities in the Reliability Program Plan are performed in an iterative manner for both a given product and for a family of products. Therefore, the follow-on products in a family of products may have well established reliability requirements for certain subsystems. The opportunities for reliability improvement may be limited largely to the new or improved components or subsystems. The RPAF activities will then be focused on these items.

3 RELIABILITY PREDICTION AND ASSESSMENT REQUIREMENTS

This heading describes implementation procedures, types of models, doneness criteria, and tools needed for the Product Team to perform reliability prediction and assessment.

The usual reason for reliability prediction is to provide a rational and quantitative basis for decision making during the conceptual design and early production phases of a product. Since reliability prediction is a forecast of reliability performance, the decisions are re-evaluated as actual reliability performance is observed.

Reliability assessment deals with parameter estimates, but must also determine whether the assumptions about the model are justified. The feedback loop revises the reliability prediction and assessment models based on the comparison of the prediction and assessment results.

Different methods and approaches are applicable, depending upon the stage of product design and the available information.

3.1 GENERAL REQUIREMENTS

Reliability predictions and assessments shall be based on the latest information on the product design, performance, behavior, environment, or other factors that affect the reliability of the product. The predictions and assessments shall be updated to reflect any changes in these factors.

Product designers and reliability engineers shall agree on the approaches, assumptions, and requirements, for reliability prediction and assessment.

The typical steps in the process of reliability prediction and assessment are the following:

1. Formulate the prediction (assessment) problem as a model.
2. Define the method for validating the model.
3. Define the doneness criterion.
4. Plan the collection, analysis, and validation of reliability data, if applicable.
5. Perform the prediction (assessment).
6. Validate results.
7. Use the results to make decision(s) or plan the next step.
8. Satisfy the doneness criterion or perform another iteration of the above process.

The reliability prediction and assessment activities shall be closely coordinated with related program activities to ensure consistency, efficiency, and accuracy. This includes ensuring all data bases are updated.

The assumptions shall be specified and documented. Approaches and assumptions may be changed, modified, or deleted if requirements change. In some cases, the assumptions are based on a rationalization of product knowledge, and this may necessitate the development of sensitivity analyses.

The reliability prediction and assessment activities have practical limitations depending on the available data, the design complexity, and the product knowledge.

Throughout the reliability prediction and assessment, validations shall be performed on the data, the input and output parameters, and on the structural and behavioral aspects of the model(s).

3.2 RELIABILITY MODELING

Formulation of the model(s) includes defining the setting and the terms, identifying the metrics, listing and validating the factors (behaviors), listing and validating the assumptions, and specifying the model parameters.

The setting for the prediction or assessment shall be defined.

The environment includes:

Temperature
Humidity
Vibration
Electrical and mechanical stresses

The structural aspects include:

Architecture (hardware and software)
Configuration

The temporal aspects include:

Age
Release version (hardware and software)

The application aspects include:

Application software
Usage patterns

The human factor aspects include:

The impact of operators and system managers on failure and recovery behavior through maintenance procedures and operator coverage

The reliability model(s) shall be developed for components, options, and systems. Each reliability model shall include documentation of all assumptions and constraints that influenced the selection of the model and all subsequent analysis. The model(s) shall be updated when there are changes in the product design, performance, behavior, environment, or other factors that affect the reliability of the product.

The reliability model shall be developed to the level of detail required by design engineers or to the extent of information that is available.

The failure and recovery behaviors shall be identified. The observed behavior shall be face validated with expert(s).

The solution of the models yields the reliability prediction or assessment. The input and output parameters for the reliability model(s) shall be consistent and compatible. The output parameters shall include the terms used in the specified reliability requirements and other reliability terms as appropriate.

3.2.1 Hardware Failure Rate

Hardware (permanent) failure rate prediction (assessment) model(s) shall be developed and maintained for those phases of product life, early life, steady state, and wearout, as they apply to the product under evaluation.

The early life failure rate models for nonrepairable items includes the Weibull distribution. For repairable items, the failure rate models include the Non Homogeneous Poisson Process (NHPP) with Weibull or the Chance Defective Exponential (CDE). This assumption is reasonable when the repaired assembly failure rate represents a small percentage of the overall system failure rate. Renewal models are used for repairable systems, where the repaired system failure rate is much different from the system failure rate just prior to the repair.

The traditional steady state failure rate model is the exponential distribution. The exponential is a special case of the more general Weibull distribution. The steady state is the only case where a distribution can be used to model both repairable (Homogeneous Poisson Process) and nonrepairable items.

The wearout failure rate models for nonrepairable items include the Weibull, the Log-Normal, and the Normal distributions. The NHPP (with Weibull, Log-Normal, or Normal intensity function) and renewal models are used for repairable items.

The Bayesian approach can be used when prior information is available (for example, information on similar products). In the Bayesian approach, the known prior parameters and the distribution for unknown prior parameters need to be specified. Very few failures are observed during the test or experiment time for long-life items. The Bayesian approach or accelerated life test can be used for long-life items. To use the accelerated life test approach, it is required to specify in advance the functional relationship between the parameters of the failure distribution and the applied stress. Example relationships include the Arrhenius Law and the Power Law. There also **must** be an understanding of the different effects that the stress levels can have on the failure mechanisms.

Generic Steps

The generic steps in the process of hardware failure rate prediction or assessment are the following:

1. Define the system, options, and components using engineering specifications, bills of materials, and architectural diagrams.
2. Define the modeling assumptions.
3. Develop the input data file and output report files.
4. Perform the prediction (assessment) of hardware failure rate.
5. Develop fault avoidance impact analyses for different design alternatives.
6. Validate hardware failure rate data for accuracy, completeness, and applicability.
7. Compare hardware failure rate prediction (assessment) with the specified early life, steady state and wearout failure rates defined in the reliability portion of the product's engineering specification.

If the prediction or assessment results are significantly different from the specification, then the reasons for the difference, and the directions for improvements shall be identified.

3.2.2 Interruption Rate and Availability

The models for interruption rate and availability take into account additional factors beyond the hardware failure rate models addressed in the previous section.

Hardware related interruptions include hardware permanent failures, and transient and intermittent events. Hardware interruptions can be bunched in time due to a common cause (resulting from the inability to diagnose the problem the first time the event is observed). The branching Poisson Process is a conceptual model of the bunching of events.

Software related interruptions will depend on the application and usage patterns (time of day). There are software models in the literature.

Site-caused environmental interruptions include power failures, network problems, temperature (as in hardware), and disasters.

Operator and other human factor-related interruptions include operator error, upgrades, reconfiguration, and maintenance policies. These may depend on time of day patterns.

Availability prediction or assessment includes both interruption rates and recovery behavior. The additional factors to consider for availability include the following:

a. Countable versus noncountable interruptions (for example, those that the user expects and will tolerate, such as preventive maintenance and upgrades).

b. The spectrum of availability ranges from minimum requirements to full availability. A system may be partially available due to unavailable (redundant) resources and degraded performance during recovery.

The setting shall be defined for the interruption rate and availability models. The definition of an interruption is often subjective due to the variety of possible settings.

Modeling shall include the distribution or distributional characteristics for time between interruptions and recovery times. Temporal patterns shall be considered. Interruption rates and availability can be modeled using the approaches described below.

Traditional Approach

The traditional analytical models for interruption rate and availability prediction or assessment are based on combinatorial methods assuming that the system is composed of a series of independent subsystems. Each subsystem is solved separately. The interruption rate and availability for the subsystems are then merged combinatorially to predict or assess the system interruption rate and availability.

Fault Tree Model

One of the traditional combinatorial methods is the fault tree model. A fault tree is a model that graphically and logically represents the various combinations of events occurring in a system that may lead to system interruption and unavailability.

Markov Model

Markov methods use continuous-parameter Markov Chains, in which a state typically represents the number of operational components of the system. The interruption rate and availability of the system is solved as the sum of the probabilities for operational states in Markov state space diagrams.

Extended Stochastic Petri Nets

The Extended Stochastic Petri Net (ESPN) is used as an aid in modeling complex fault and error-handling system behavior. A Petri Net is an abstract and formal graph model useful for representing systems that exhibit concurrent, asynchronous, or nondeterministic behavior. The Petri Net generates a Markov model that can be solved using the tools described in Section 3.8.

3.2.2.1 Fault Occurrence and Error-Handling Submodels

Markov models for complex systems often suffer from having a large state space. To solve the large state space problem, decomposition and aggregation methods are used. Decomposition and aggregation are the complementary activities of separating and combining parts of the system to facilitate model formulation and solution.

The two ways to decompose the system to solve the large state space problem are called structural and behavioral decomposition.

The most common solution consists of structurally (physically) dividing the system into smaller subsystems, solving the subsystems separately, and then combining the subsystem solutions to obtain the overall system solution. If the subsystem fault-tolerant behaviors are mutually independent (or can reasonably be assumed to be independent), then a decomposition into subsystems can be used. The applicability of the structural decomposition approach diminishes as systems become more highly integrated.

With behavioral decomposition, it is observed that faults may occur over periods of weeks or years, for example, but detection and recovery may only take seconds. It is desirable, therefore, to decompose along temporal rather than structural lines. In this way, the fault- and error-handling behavior can be separately analyzed, and the result of analysis can in turn be used in an aggregated model. Therefore, it is possible to use different model types and solution techniques for the submodels.

The overall interruption rate and availability model is decomposed into fault occurrence and repair, and fault-handling and error-handling submodels. The fault occurrence and repair model contains information about the structure of the system redundancy, and about the fault arrival and repair processes. These submodels are specified and solved separately, and are then combined to obtain the solution for the overall system.

3.3 FAILURE DATA SOURCES

The following sections describe sources of prediction information.

3.3.1 Prediction Data

Different sources of information are available for component failure rates. The major sources are the Digital Reliability Estimates and Methods (DREAM) [4] and the industry standard, MIL-HDBK-217 [5]. These sources contain component failure rate estimates and methods for predicting the failure rate for subassemblies through systems before actual manufacture and use.

The data for interruption rate and availability prediction generally are obtained from observed behavior of Digital systems, products and services, or from estimates obtained from Digital experts. The scarcity of this data, and the many sources of variability, often necessitate the use of sensitivity analyses in the prediction procedure.

The data for interruption rate prediction includes the component failure rate data, intermittent hardware faults, software faults, environmental faults, and human faults.

The availability prediction includes data for the interruption rate, fault-handling, error-handling, and recovery behavior associated with each fault type.

3.3.2 Data Collection Considerations

Planning the data collection and analysis shall include considerations of precision, environment, confidence, sample size, sample homogeneity, duration of test or experiment, tools for accuracy and efficiency, real-time control of the test or experiment, logistics, and people involvement.

The data sources shall be evaluated regarding the usefulness of the data with respect to accuracy (gaps, detail), impartiality (correctness of the recording of the data), and representativeness. The tradeoffs shall be considered in obtaining better data.

The data collection and analysis plan shall describe how to extract, filter, manage, and report the data, and how to test any tools developed.

Limitations in the interpretation of the data are considered and validations are carried out, as necessary.

Data collection, analysis, and validation issues may be greater for interruption and availability prediction (assessment) because there are more sources of variability, less control over the setting, and because the setting changes over time.

3.4 PREDICTION AND ASSESSMENT PROCEDURE

The following steps define the procedure for developing failure rate, interruption rate, and availability prediction or assessment:

1. Define the product for which the prediction (assessment) is required using product and market application descriptions, where applicable.
2. Identify market requirements for failure rate, interruption rate, and availability, and allocate the requirements to systems, options, and components, where applicable.
3. Define the component, option, and system reliability block diagrams for each product configuration, using engineering specifications, bills of materials, and architectural diagrams.
4. Define all factors that contribute to failure rate, interruption rate, and availability prediction (assessment), including operating environment usage factors.
5. Define the mathematical models for predicting failure rate, interruption rate, and availability, where applicable.
6. Define the structural and behavioral parameters and assumptions.
7. Compute the hardware failure rate, interruption rate, and availability, where applicable,
8. Determine the effectiveness of fault avoidance and fault tolerance approaches.
9. Compare the predictions (assessments) with the requirements and determine the reasons for the differences.

A typical list of parameters used in hardware failure rate, interruption rate, and availability prediction modeling are the following:

- Reliability parameters
  - — Hardware failure rate parameters for infant mortality, steady state, and wearout, that apply to the product under evaluation
  - — Permanent/intermittent failure rate ratio
  - — Listing of single points of system failure
  - — Listing of critical components
  - — Rates of other sources of interruption
- Maintainability parameters
  - — Hardware repair rate
  - — Maintenance personnel travel time
  - — Preventive maintenance strategy
  - — Number of repair personnel

- Complex system behavior
  - — Fault detection rates
  - — Fault isolation rates
  - — Fault coverage rates
  - — Recovery rates
  - — Degraded performance parameters and so forth

3.5 DONENESS CRITERION

The prediction or assessment shall be considered done and when agreement has been reached among the Product Team and the results are documented.

3.6 TOOLS

This section describes the tools available to determine hardware failure rate prediction and assessment.

3.6.1 Hardware Failure Rate Prediction

Computer programs are available for hardware failure rate prediction in the early life and steady state periods.

Computer Aided Design Reliability Engineering (CADRE) [6] is a computer program for prediction in both the early life and steady state periods, and also is an automated system that provides permanent database storage and retrieval of component lists, component specifications and failure rate data. The CADRE operating environment parameters can be selected or modified (for example, to use DREAM or other sources of failure rates, ambient or junction temperature, sort keys for output report generation, and so forth). The modular export routines create the necessary text and data files to be used as input to other packages, such as to interruption rate and availability modeling.

PREDIC [7] is an interactive computer program for steady state failure rate and MTBF prediction in accordance with the methods in MIL-HDBK-217. Since PREDIC has built-in default values for all prediction parameters, it is possible to use the program with very limited knowledge. However, to obtain an accurate prediction, suitable for design tradeoff studies, it is essential to have a working knowledge of the failure rate models and MIL-HDBK-217 techniques. Refer to *PREDIC Reliability Predictions Users Manual, EL-EN418-00*.

Screen Debugging Optimization (SDO) is a software tool for modeling the process reliability and associated test and repair costs. As more precise data becomes available, SDO may be rerun until it has been calibrated to the specific process. It can compare actual and predicted parameters. Contact Ed Hoover, Chief Engineer's Office (see VTX ELF for location information).

3.6.2 Hardware Failure Rate Assessment

There are currently two Digital supported software packages for hardware failure rate assessment. These packages are VAX Reliability Tools Suite (VAXRTS) [8] and exponential Probability Ratio Sequential Test (PRST) [9]. Recently, subpopulation hardware failure rate assessment methods have also been applied in Digital. There also are several commercial packages for assessment.

VAXRTS provides procedures to analyze data for repairable and nonrepairable systems. The program can calculate needed sample sizes for a test of fixed length. VAXRTS also provides parameter estimation and goodness of fit for the NHPP with Weibull intensity function or the Weibull distribution. If past knowledge is available for the product, VAXRTS also provides Bayesian estimation techniques for the above mentioned models.

The SPRT program provides a procedure for developing an exponential distribution sequential probability ratio test similar to the methods given in MIL-HDBK-781 [10]. The program generates the minimum test time with zero failures, and the truncation time when the test must end.

3.6.3 Interruption Rate and Availability Prediction and Assessment

The application of the tools for interruption rate and availability prediction and assessment, and the interpretation of the results, requires a great deal of user expertise and sophistication.

Sophisticated tools have been developed in Digital to assist in the analysis of interruption rate data from system error (event) logs, operator (OPCOM) logs, and Labor Analysis and Reporting System (LARS) data. The tools include Crash Rate (CRATE), European Systems Reliability Information (ESRI) [11], and several development tools. These tools differ in the sources of interruption rate data used and in the level of application (cluster versus machine level). The tools have been described and compared in a survey paper [12].

State of the art tools for interruption rate and availability assessment and prediction have been brought into Digital from the industry. These are the Stochastic Petri Net Package (SPNP) [13], the Symbolic Hierarchical Automated Reliability and Performance Evaluator (SHARPE) [14], and the Hybrid Automated Reliability Predictor (HARP) [15]. These tools assist in the formulation of the model(s) and provide sophisticated solution methods for very large models.

APPENDIX A REFERENCED DOCUMENTS

A.1 EL-Class Digital Documents

EL-Class Number	Document Title
EL-EN418-00	*Predic Reliability Predictions Users Manual*
EL-EN522-00	*Digital Qualification Process Manual*
EL-EN522-01	*Storage Systems Qualification Manual*

Use VTX SMC to order copies of EL-class documents from Standards and Methods Control. Send distribution questions to JOKUR::SMC or call DTN: 234-4423.

A.2 Other Digital Documents

Document Number	Document Title
EA W0122-85	*Digital Quality Systems*

APPENDIX B RELATED DOCUMENTS

B.1 EL-Class Digital Documents

EL-Class Number	Document Title
EL-00009-02	*DEC STD 009-2 Product Engineering Specifications: Reliability, Availability, and Maintainability Parameters*

Use VTX SMC to order copies of EL-class documents from Standards and Methods Control. Send distribution questions to JOKUR::SMC or call DTN: 234-4423.

B.2 Other Documents

Document Number	Document Title
MIL-HDBK-217E	*Military Handbook - Reliability Prediction of Electronic Equipment*
MIL-HDBK-781	*Reliability Design Qualification and Production A Tests: Exponential Distribution*

B.3 Ordering Information

Following are the sources for documents not available from Standards and Methods Control.

- Federal Standards, Military Standards, Naval Publications, and Forms Center:
  5801 Tabor Avenue
  Philadelphia, PA 19120
  Telephone (215) 697-3321

APPENDIX C BIBLIOGRAPHY

Following are the documents that supply additional information:

1. Reliability Advisory Committee, *Designing for Reliability in Computing Systems - A Generic Plan*, June 1986.
2. Reliability Advisory Committee, *Digital Qualification Process Manual*, A-MN-ELEN522-00-0 Rev A, September 1989, *and*
3. *Storage Systems Qualification Manual*, A-MN-ELEN522-01-0 Rev B, July 1990.
4. *DREAM: Digital Reliability Estimates and Methods Notebook*, Rev 2.0, June 1989.
5. MIL-HDBK-217E, *Military Handbook—Reliability Prediction of Electronic Equipment*, October 1986.
6. Systems Reliability Engineering, *CADRE - Phase 3, Computer Aided Design Reliability Environment Functional Specification*, October 1989.
7. Chief Engineer's Office, *PREDIC, Reliability Prediction User Manual*, November 1986.
8. Systems Reliability Engineering, *VAX Reliability Tools Suite User Guide V 1.2*, January 1990.
9. *Exponential SPRT Generator Specification*, A-MN-ELEN036-00, Rev C2, June 1989.
10. MIL-HDBK-781, *Reliability Design Qualification and Production A Tests: Exponential Distribution*, July 1987.
11. Moran, Pat, Gaffney, Pat, and Melody, John, *System Availability Monitoring*, ESASE Group, Proceedings of the First Digital Reliability Seminar, October 1989.
12. Card, Jill, *Cross Community Crash Rate Data Collection and Analysis*, Reliability Advisory Committee, June 1989.
13. Ciardo, Gianfranco, Muppala, Jogesh, Trivedi, Kishor, *SPNP : The Stochastic Petri Net Package Introduction and Guide for User, Version 3.0*, Duke University, Durham, NC, December 1989.
14. Sahner, Robin A. and Trivedi, Kishor S., *SHARPE: Symbolic Hierarchical Automated Reliability and Performance Evaluator Language Description*, Duke University, Durham, NC, December 1989.
15. Rothmann, Elizabeth, Dugan, Joanne B., Trivedi, Kishor S., and Mittal, Niti *HARP : The Hybrid Automated Reliability Predictor Introduction and Guide for Users, Version 6.1*, Duke University, Durham, NC, January 1990.

GLOSSARY

allocation: The process of distribution of the quantitative reliability characteristics (goal, requirements, prediction) between systems, options and components.

assessment : The process of determining the achieved level of reliability of an existing system, option, or component.

availability : The probability of delivering the service as specified, under stated conditions, at a stated instant of time. In the limit as time approaches infinity, availability is the fraction of time the service is delivered as specified.

component : A part of a system or option.

database : A set of information quantitatively describing system, option, or component reliability.

goal : A desired result.

early life period : A period that occurs during the initial life phase of a system, option, or component. This period is characterized as a period of decreasing failure rate.

metric : A characteristic used in measurement (for example, failure rate, interruption rate, down time per year).

option : A part of a system that is saleable (for example, memory, disk drive).

prediction : The process for determining the expected level of reliability.

product : An entity produced for delivery to a customer or user (for example, option, system, cluster, application software).

reliability : The probability of continuously delivering service as specified under stated conditions for a stated period of time.

requirement : An essential result.

service interruption : An unscheduled event which results in the disruption of service and loss of work to a user or class of users.

specification : A document that delineates the product requirements or other characteristics of a system, option, or component.

steady state period : A period that occurs during the ongoing life phase of the system, option, or component. This period is characterized as a period of constant failure rate.

system : A group of options and components that are united and function as a single unit.

unavailability : The complement of availability ($1 - Availability$).

validation : The process of evaluating to ensure compliance with requirements.

wear-out period : A period which occurs after the steady state phase of a system, option, or component. This period is characterized as a period of increasing failure rate.

Fault Occurrence and Error-Handling Terminology

error : An incorrect response from a hardware or software component. An error is a manifestation of a fault.

failure : The inability of a system, option, or component to provide a required service under stated conditions.

failure rate : The number of failures for a given unit of measure.

fault : Erroneous state of hardware or software resulting from failures of components, physical interference from the environment, human error, incorrect design or manufacturing, improper repair or maintenance.

hard (permanent) failure/fault/error : A failure, fault, or error that is continuous or stable. It requires a physical repair of the system, option, or component (in a case of hardware) or recoding (in the case of software). The hard failure or fault or error can be reproduced.

intermittent failure/fault/error : A soft failure, fault, or error resulting from unstable hardware or software.

soft (temporary) failure/fault/error : A failure, fault, or error that is only occasionally present due to unstable system, option, or component conditions. It does not require a physical repair of the system (in the case of hardware) or recording (in case of software). It cannot be reproduced. It can be recovered from or by a system, option, or component, reboot or retry.

transient failure/fault/error : A soft failure, fault, or error resulting from environmental conditions.

```
+-------------------------------------------------------------------+
|                        READER COMMENTS                            |
|                                                                   |
| Your  comments  and suggestions  will help  Standards and Methods |
| Control improve their services and documents.                     |
+-------------------------------------------------------------------+
```

Did you request this document? _____ If so, did it arrive within a satisfactory period of time? _____ Please comment.

What are your impressions of this document? Consider format, organization, completeness, readability, and illustrations.

————————————**FOLD ON THIS LINE**———————————————————————— -

Did you find technical or clerical errors in this document? If so, please specify the page number(s) and the error(s).

Are the instructions for the update package clear? _____
Was an index available? _____ If not, is one needed? _____
Do you have other suggestions for improving this document?

The following information is optional:

Name _____ Mailstop _____

Department _____ Node _____

Send your comments to JOKUR::PROJECTS, or fold, staple, and send this page through interoffice mail to:

```
+------------------------------+
|       READERS' COMMENTS      |
| STANDARDS AND METHODS CONTROL |
|           NRO4/D4            |
+------------------------------+
```